

LEGAL FOUNDATIONS

STUDIES AND CONCLUSIONS

Report 1 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997



This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Contents

	Page
Acknowledgments	iii
Preface	iv
Part One: Legal Activities	1
The Federal Legal Landscape.....	1
The Regulatory Landscape	4
Legal Authorities Database.....	4
Infrastructure Protection Solutions Catalog	6
Part Two: Legal Issues	7
Major Federal Legislation	7
Adequacy of Criminal Law and Procedure (Cyber)	8
Adequacy of Criminal Law and Procedure (Physical)	8
Privacy Laws and Employer-Employee Relationship	8
Legal Impediments to Information Sharing.....	9
Federal Government Model Performance	9
Approaches to Cyber Intrusion Response	9
Part Three: Conclusions	10
Enabling the Federal Government to Take the Lead	11
Enabling Private Sector Response.....	20
Enabling Government-Industry Partnership.....	24
Part Four: Infrastructure Assurance, Law and Culture	28

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President’s Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the

possible approaches and conclusions that were presented to the PCCIP for its consideration. The series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Part One

Legal Activities

With Executive Order 13010, the President’s Commission on Critical Infrastructure Protection (PCCIP) was tasked to assess the vulnerabilities of, and threats to, eight named critical infrastructures, and also to develop a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required the Commission to consider the legal and policy issues raised by efforts to protect the critical infrastructures and to propose statutory and regulatory changes necessary to effect potential Commission recommendations. The results of these efforts are documented in the 12 reports that constitute the *Legal Foundations* series.

The first part of this summary report describes the legal survey work done to better inform the PCCIP about the complex webs of legal and regulatory authorities surrounding each of the critical infrastructures, and documents the methodology used to identify legal issues and generate material for potential recommendations. It also contains a summary of the substantive legal work that further informed the Commission's efforts.¹

The first step characterized the legal and regulatory “landscapes”—providing overviews of the legal and regulatory climates surrounding each of the critical infrastructures. This initial landscaping project, and the difficulties inherent in adequately capturing legal authorities relating to the protection of critical infrastructures, stirred the undertaking of several other activities and the creation of a number of products. The following sections capture the results of these efforts.

The Federal Legal Landscape

The landscape process began by surveying attorneys from the offices of General Counsel from the ten agencies represented on the Commission: the Departments of the Commerce, Defense, Energy, Justice, Transportation, and Treasury; and the Central Intelligence Agency, Federal

¹ The legal materials presented have been compiled only from publicly available materials. The *Legal Foundations* series of reports contains statements of the law and legal analysis. While there are classified materials that are relevant to the legal issues associated with infrastructure assurance, they have not been included within the scope of these materials.

Bureau of Investigation, Federal Emergency Management Agency, and the National Security Agency. The General Counsel attorneys were briefed on the goals and objectives of the PCCIP. They, in turn, provided the Commission with accounts of their agencies’ legal authorities and mechanisms relating to infrastructure assurance.

To aid those efforts, the Commission provided the survey matrix shown in Figure 1 below. The matrix breaks down “infrastructure assurance” into the components of the three-part definition from the report of the Critical Infrastructure Working Group (CIWG), a definition that has continued to serve well through the Commission’s efforts. Infrastructure assurance is defined as “...the surety of readiness, reliability and continuity of infrastructures such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be readily reconstituted to reestablish vital capabilities.” The matrix encourages further analysis by specific critical infrastructure and purpose of the authority (i.e., legal authority or enforcement mechanism, physical or cyber threats). The General Counsel attorneys were also encouraged to identify plans and projects “under construction” that appeared to relate to assurance efforts and to suggest other agencies with stakes in infrastructure assurance efforts.

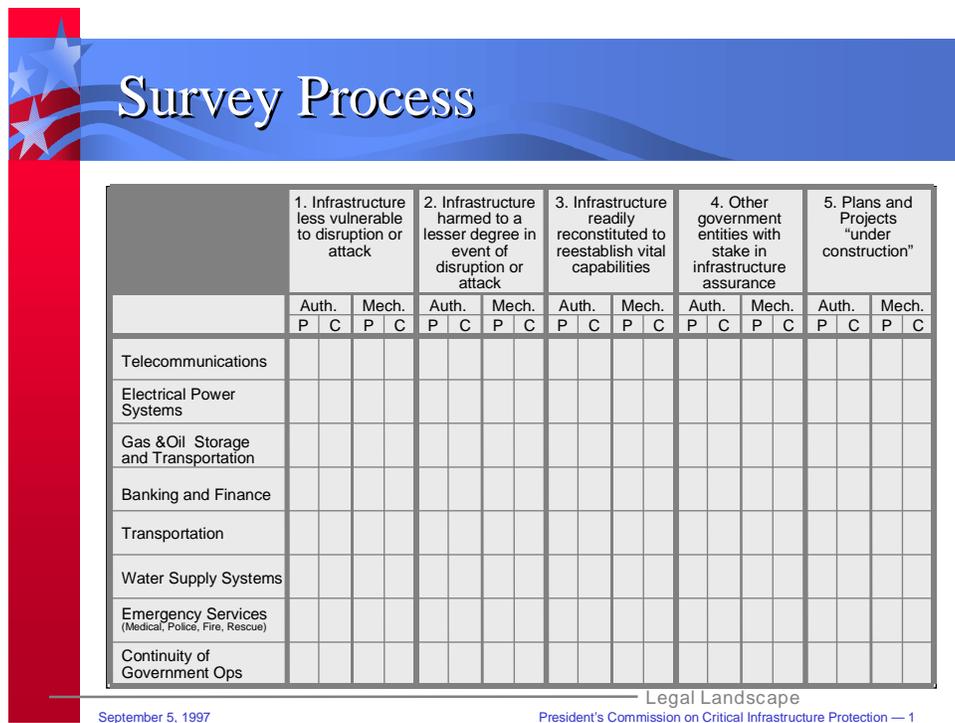


Figure 1: Infrastructure Assurance Authorities Survey Matrix

From the preliminary results of the survey effort, it became apparent that to achieve a reasonably complete picture of the Federal government’s authorities and mechanisms that could be used to achieve infrastructure assurance objectives, a broader outreach effort would be needed.

Additional agencies were identified and contacted. The agencies that participated in the Commission’s legal outreach activities are depicted in Figure 2, below.

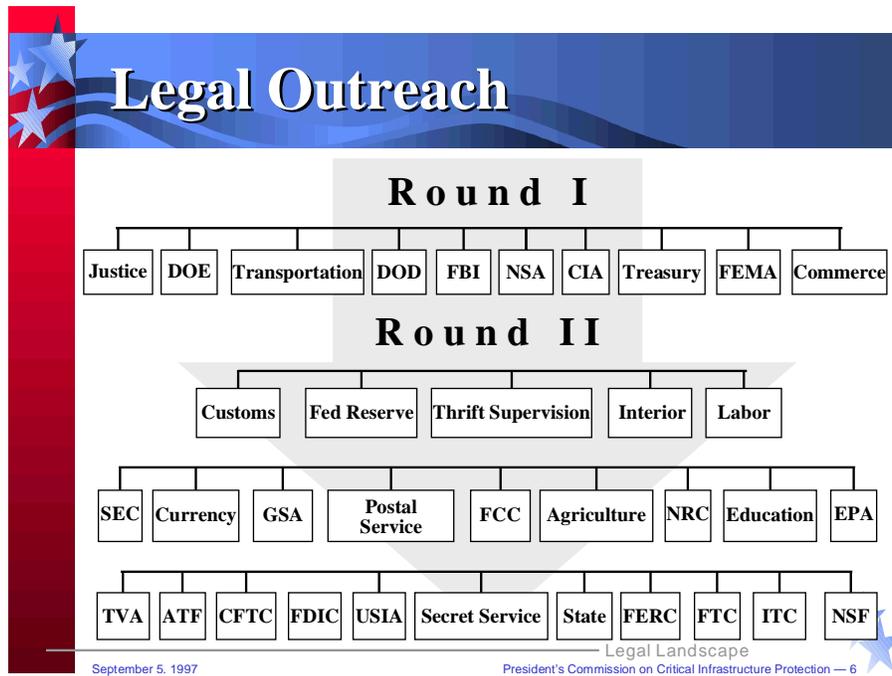


Figure 2: Legal Advisory Group Representatives

Representatives of these thirty-five agencies comprised the PCCIP Legal Advisory Group, a body that provided a sounding board for potential Commission recommendations. Their submissions were studied, supplemented, summarized and compiled into a report on the pertinent legal authorities of the Federal government.

The study, *The Federal Legal Landscape*, is a high-level overview to provide the reader with a picture of the Federal laws, regulations, and structures that exist within each critical infrastructure and within each participating agencies’ sphere of authority. It is essentially a roadmap to the Federal government’s infrastructure assurance authorities, offices and capabilities. Those who have attended meetings of the Legal Advisory Group or who have otherwise participated in the preparation of submissions are listed in Appendix A of *The Federal Legal Landscape*.

The Regulatory Landscape

In addition to *The Federal Legal Landscape*, which focuses primarily on broad authorities possessed by the Federal government, the Commission felt that a study of the current and past regulatory climates of the critical infrastructures would be very helpful. Historically, the critical infrastructures differ in the degree to which they have been regulated, and the reasons for their continued regulation. Some were regulated predominantly by concern for broad access to service, while others were regulated over matters relating to market power, public safety, or consumer confidence. With restructuring occurring across some of the critical infrastructures—results of efforts to open markets and increase competition—they now also differ in the extent to which they are being restructured. Potential impacts on security and reliability were areas of concern and study. A study of the regulatory landscape, titled *The Regulatory Landscape* was undertaken to provide a better understanding of the way regulatory tools and mechanisms—Federal, state, local or private—are being, or could be used to promote infrastructure assurance objectives.

Legal Authorities Database

The Legal Authorities Database is an outgrowth of various “landscaping” projects. The Commission recognized early on that, given methodological and time constraints, the landscaping efforts could not reasonably be expected to capture, for example, the full range of international bodies, treaties, and conventions relevant to the infrastructures or infrastructure assurance. Nor would these landscaping efforts adequately account for or explain “authorities” that—although not promulgated by governments per se—nonetheless can be influential in effect. We refer here to the myriad policies, guidelines, and standards (such as auditing standards) that carry force of law for private sector and public sector owners and operators of critical infrastructures. Neither the legal nor the regulatory landscape, separately or together, would provide a complete panorama of legal authorities associated with infrastructure assurance, nor would they provide an adequately broad picture of relevant cross-infrastructure issues.

The legal and the regulatory landscapes do a good job of capturing many legal authorities relating to infrastructure assurance, which as a result, may be used to *promote* or *enhance* infrastructure assurance. Some current laws, regulations, policies, or guidelines, however, may actually operate in ways that are *antithetical* to achieving infrastructure assurance objectives. Identifying,

reviewing, understanding and revising those authorities in appropriate ways may prove to be as valuable as creating new ones.

To fill this void, the Commission recruited a team of attorneys to cull through the United States Code, the Code of Federal Regulations, Executive Orders, treaties, select state legislation and other relevant authorities with “infrastructure assurance” in mind. The authorities found to bear on infrastructure assurance—positively and negatively—were then incorporated into a database. The database was originally built around key words and concepts relevant to assurance efforts. These included topics such as indications and warning, information sharing, education and awareness, information security, emergency response and others. (Although the database, now with over 14,000 entries, has grown beyond these topics, these keywords and concepts continue to serve as useful search terms to guide research efforts.) The database represents a source of data which could facilitate implementation of PCCIP recommendations by Federal, state and local governments and by the private sector.



Figure 3: *Legal Authorities Database CD Cover*

Infrastructure Protection Solutions Catalog

The *Infrastructure Protection Solutions Catalog* is a compendium of prior recommendations made by informed individuals, study commissions, and other groups who have weighed in on issues related to the Commission's work. This document contributed not only to the identification of possible legal issues, but also served as a validation that a number of broad solution areas were adequately explored.

Part Two

Legal Issues

The Commission was asked to identify legal and policy issues raised by efforts to protect the critical infrastructures, and to make recommendations for reform. Studies were undertaken to identify relevant issue areas.

Originally, some 16 discrete issue areas were identified, but later consolidated to seven.² These issue areas focus not only on using existing authorities to promote infrastructure assurance objectives (e.g., through greater inclusion of cyber concerns into existing statutes), but also on the need to remove existing legal impediments to infrastructure assurance-related actions. Results captured in the following studies in the *Legal Foundations* series reflect the significant background research completed to support the Commission's work.

Major Federal Legislation

This study explores major areas of Federal legislation, such as the Defense Production Act of 1950, the Stafford Act/Federal Response Plan, the Computer Security Act of 1987, the War Powers Resolution and related authorities, and the Nunn-Lugar-Domenici legislation. It reviews whether these evolving bodies of authority appropriately take into account threats to the critical infrastructures. It also addresses whether these authorities could be considered for modification to better address physical and cyber threats, or whether separate legislation would be preferable for this purpose.

² Of these, liability was addressed as an economic issue by the Commission to insure that it would be considered not only from a legal perspective, but from a broader economic perspective as a tool for social change.

Adequacy of Criminal Law and Procedure (Cyber)

This study explores the adequacy of Federal and state substantive criminal law to deter and punish those who commit computer-based attacks on critical infrastructures. It also evaluates procedural law, and whether it may place undue impediments on law enforcement's ability to conduct investigations.

Adequacy of Criminal Law and Procedure (Physical)

This study explores the adequacy of criminal law to respond to and deter physical attacks on critical infrastructure.

Privacy Laws and the Employer-Employee Relationship

This study looks at laws that prohibit or restrict infrastructure owners and operators from making use of various devices and processes routinely used by the Federal government in conducting background investigations and issuing security clearances to employees in highly sensitive positions. It explores the balance between concerns over security and privacy.

Legal Impediments to Information Sharing

This study attempts to forecast the various legal impediments that might inhibit the flow of infrastructure assurance-related information between and among government bodies and the private sector. It suggests ways in which an information sharing mechanism might be structured to minimize these legal impediments.

Federal Government Model Performance

This study explores five discrete areas through which the Federal government can unilaterally alter its own behavior in order to encourage the private sector, state or local governments to act consistently with infrastructure assurance objectives. They include performance measurement; publication of infrastructure assurance-related data; identification and dissemination of “best practices,” procurement reform; and certification programs.

Approaches to Cyber Intrusion Response

This study assumes that the number and severity of computer intrusions will continue to grow, and that a conventional law enforcement response might not be sufficiently robust to maximize deterrence. It explores viable alternatives to traditional criminal enforcement mechanisms (investigative and prosecutorial) to serve as a supplemental deterrent to unauthorized computer intrusions.

Part Three

Conclusions

An overarching and unsurprising conclusion from the *Legal Foundations* series of studies is that law has failed to keep pace with technology. Some laws capable of promoting infrastructure assurance objectives are not as clear or effective as they could be. Still others can operate in ways that may be adverse to security concerns. Sorting them all out, of course, will be a lengthy and massive undertaking, involving efforts at local, state, Federal, and international levels. The studies within the *Legal Foundations* series represent a jump-start to a possible process of reform.

The conclusions presented in this paper reflect a principled approach to achieving infrastructure assurance. They reflect efforts to assess and understand the legal and regulatory landscapes of the critical infrastructures; the work of prior bodies (and the courses of action they recommended); and research on pressing legal issues that emerged from supporting the Commission's efforts. Much of the legal work presented throughout this series of studies examines the operation of the laws and regulations within and across the critical infrastructures at a micro-level. This following section collects observations and conclusions, so as to place them into a larger perspective—as a series of attainable steps to lay the legal foundation for the processes and mechanisms that should be considered in efforts to achieve continued assurance of the critical infrastructures.

The Process of Infrastructure Assurance

“Infrastructure Assurance” is not merely an end state, but a continuous process. It is a process of continuing to improve capabilities in five general areas: (1) policy formulation; (2) prevention and mitigation; (3) operational warning; (4) incident management; and (5) consequence management.

Responsibilities in these areas are performed today to varying degrees within each of the critical infrastructures by the Federal government, state and local governments, trade associations, and by individual owners and operators of critical infrastructures. "Legal Activities" described in *The Federal Legal Landscape* and *The Regulatory Landscape* revealed shortcomings of current efforts. First, current efforts are largely uncoordinated. Infrastructure regulators (Federal and state), law enforcement, intelligence, emergency preparedness and management, defense and other communities formulate policies that control the security and reliability of the critical infrastructures, but they do so by-and-large independently. Second, vital information is not

currently shared between and among infrastructure sectors, and between and among government in ways that would feed a more complete understanding of the risks facing the critical infrastructures. Policy and information are developed and held in pockets which do not come together to be analyzed and de-conflicted.³

Roles of the respective parties in infrastructure assurance should periodically be reevaluated and redefined to reflect the new environment in which the critical infrastructures will operate. Recommendations for organizing a national infrastructure assurance effort will, by necessity, reflect the need for new roles—greater private sector participation in policy formulation, effective information sharing between and among government and the private sector, and greater sharing of resources for research and development. Many of the conclusions presented here are intended to enable these roles to be undertaken by those most suited to the task.

Legal Foundations Conclusions

The conclusions drawn from *Legal Foundations* are designed to jump-start the gradual process of reform. They are set forth in three parts. Existing laws can be made to better serve the government in an effort to take the lead and serve as a model of standards and practices for the private sector. Other areas of law, with careful attention, can enable infrastructure owners and operators to take precautions proportionate to the threat. Still other areas of law can be molded to enable a greater degree of government-industry partnership in areas such as information sharing. Many of these proposals call for further study of areas deserving additional attention.

Enabling the Federal Government to Take the Lead

Achieving increased protection depends on voluntary cooperation. In order to attract it, government must demonstrate its own commitment to the protection of the critical infrastructures and lead by example. The first set of conclusions presents several ways the Federal government

³ Not only is policy uncoordinated and vital information unshared under the current construct, but the focus within few of these functional areas is on “infrastructure assurance.” Regulators are primarily concerned with safety and reliability; owners and operators with competitiveness and growth; law enforcement with prosecuting criminals; intelligence with gauging threats; defense on preparing for war—these are the traditional roles of these constituencies. However, in the face of new threats and vulnerabilities, new technologies, and increasing irrelevance of jurisdictional boundaries, some of these roles may merit continued re-examination and realignment.

may better fulfill its traditional governmental responsibilities through performance-based measures, modest legislative initiatives, and by enhancing deterrence to criminal activities that threaten critical infrastructures.

Federal Government Model Performance

Model performance means measures that can be undertaken unilaterally by the Federal government, involving minimal alterations to structures, expenditures or regulations, that will enhance assurance for government and carry over positive effects for owners and operators of the critical infrastructures. Techniques such as the greater use of performance measures, publishing of comparative data, certifications, and revision of government procedures for procurement were identified and studied. (*See Federal Government Model Performance.*)

Publication of Infrastructure Assurance-Related Data

The Federal government can make use of information already in its possession to better assess threats and vulnerabilities, and to encourage others to do likewise. The publication of comparative data within an industry, such as on-time arrival and departure statistics for airlines, may serve to promote particular concerns, such as information security and reliability, without resorting to regulation. Much of this information may already be collected and may prove useful to consumers in light of increased competition and choice between providers of critical infrastructure services. Accordingly, a conclusion is that:

- The Administration could direct FCC's Network Reliability and Interoperability Council to initiate a pilot study as to the feasibility of publishing comparative infrastructure assurance-related data for the telecommunications industry. This data may be related to reliability, security or other issues identified during the course of the pilot study. The study should focus on whether publication is likely to achieve infrastructure assurance objectives; the types of data to collect and publish; whether current data collection efforts are sufficient or new ones are needed; and other possible impacts, positive and negative, of publication. The NRIC study should be followed by similar studies in other critical infrastructure sectors.

Procurement Reform

The Federal government could, where feasible, incorporate infrastructure assurance concerns into large pending procurements such as the re-competition of FTS 2000. Also, because of easy availability of waivers and other gaps in procurement policies and regulations, assurance objectives might not be adequately addressed by current procurement processes. Accordingly, a conclusion is that:

- An interagency task force could be convened to identify large pending procurements related to infrastructure assurance issues, study whether infrastructure assurance objectives are being adequately taken into account, how they may be adapted, and based on the lessons learned, suggest revisions for the procurement process generally.

Standards And Certifications

The Federal government could serve as a model for the private sector with respect to its own information security standards and compliance with those standards. Standards can provide a foundation for government-sponsored certification programs to signify compliance with security-related objectives. Some government-sponsored certification programs (for example, EnergySTAR), do not require large bureaucracies to oversee implementation and enforcement, but make available marketing incentives to encourage private sector participation. These programs place the burden of compliance principally on those who opt to use the certification. They can be inexpensive for the government to administer, and can be enforced principally through civil remedies rather than large regulatory bureaucracies. Accordingly, a conclusion is that:

- Lead Agencies can consider the creation and use of certification programs which are inexpensive to administer and enforce, and which provide incentives for adoption of standards relating to information security and information technology services and products.

Performance Measurement

The Federal government could better assess its progress in implementing these and other infrastructure assurance-related goals. Effective tools for doing so have been put in place through the “Reinventing Government” initiative. The Government Performance and Results Act (GPRA) currently requires five-year strategic plans and performance measures for major functions and operations of federal agencies. These performance measures are reviewed by OMB and Congress as part of the budget process. The Information Technology Management Reform Act (ITMRA) also requires the setting of performance measures related to the use of information technology. The required performance measures, however, do not specifically include information security. Accordingly, a couple of conclusions emerged:

- Federal agencies can be directed to include assigned roles and functions relating to infrastructure assurance specifically within their strategic planning and performance measurement framework; and

- The Information Technology Management Reform Act can be amended to specifically require agency Chief Information Officers to develop performance measures for the security of their information systems and to submit evaluations to OMB as required by the statute.

Revisiting Federal Legislation in Light of Infrastructure Assurance Objectives

Many areas of Federal legislation that enable prevention and mitigation, reconstitution, response and recovery to incidents involving the critical infrastructures were written before the emergence of a recognizable cyber threat. It is not clear whether many of these authorities would apply, and should apply, in the event of a major cyber-related event. Until the dynamics of such an event are better understood, legislative change would be premature. However, key issues were identified and conclusions reached in order to incorporate infrastructure assurance issues within these legislative frameworks. (*See Major Federal Legislation.*)

The Defense Production Act

The Defense Production Act (DPA) is an important mechanism for security of the nation's industrial and technological base. Its authorities, including priorities in contracts, financial incentives, and voluntary agreements, may assist in the reconstitution or recovery of a critical infrastructure made necessary by a physical or cyber event. The DPA authorities and triggering mechanisms, and efforts underway at modernization were reviewed to determine whether these powers might be available and adequate in light of emerging threats, vulnerabilities, and related challenges. Accordingly, some conclusions emerged:

- That the Administration and Congress could review the DPA in light of infrastructure assurance objectives; more specifically, that
 1. Congress could consider amending the DPA Declaration of Policy to include a finding of how critical infrastructures are essential to national security;
 2. Lead agencies associated with the critical infrastructures could study the energy provision for priorities in contracts as a potential model for other critical infrastructures in order to ensure continued operation and clear authority for use in reconstituting such infrastructures after an event;
 3. Funding for the DPA Fund and financial incentives could be supported and appropriated and that such funds are made available for research and development related to the critical infrastructures; and

4. The Administration could direct Federal agencies with authorities pertaining to the critical infrastructures to review the DPA's authorities and work with industry to make available such authorities when needed to respond to a critical infrastructure incident.

The Stafford Act/Federal Response Plan

The Stafford Act and the Federal Response Plan set out the parameters of the Federal response to major disasters as declared by the President. The Federal Emergency Management Agency's authority to prevent, mitigate, and respond to physical or cyber incidents affecting the operation of the critical infrastructures may require some degree of clarification or modification. Accordingly, the analysis led to a conclusion that:

- The Administration should undertake a study of Stafford Act and Federal Response Plan mechanisms to determine their applicability and suitability to cyber-induced disasters as well as their current implementation with regard to prevention and mitigation. Such a study would also take into account other disaster recovery authorities and their potential impacts on infrastructure assurance goals, as well as the desirability of providing direct assistance to infrastructure owners and operators.

The Deterrence-Related Authorities

Authorities such as the War Powers Resolution and the U.N. Charter set out conditions for use of force against nations. Many of these authorities were written before the emergence of information warfare and cyber threats. As these threats evolve, the mechanisms and policies that enable defense of our nation should be reviewed and updated to ensure they enable an adequate and effective response, and instill adequate deterrence where appropriate. Accordingly, a conclusion is that:

- The Administration, including the National Security Council and other appropriate agencies, could ensure that the U.S. strategy for responding to an information warfare attack addresses the potential legal issues associated with current definitions of "attack" contained in important domestic and international legislation.

Nunn-Lugar-Domenici

The Nunn-Lugar-Domenici legislation creates a partnership involving many Federal agencies and state and local governments to increase responsive capability to weapon of mass destruction incidents across the United States. It focuses on providing training, access to equipment, and information to local first responders. While these programs are in their initial phases, already state and local police, fire, and medical officials are requesting an expanded effort in this area. More resources for training and equipment may be required based on updated assessments of

threats, and may also require that the effort be expanded in scope to address other infrastructure-related events. Accordingly, a conclusion can be drawn that:

- Congress could consider whether the current Nunn-Lugar-Domenici program should be expanded to incorporate other critical infrastructure issues, including attacks on infrastructures by means other than Weapons of Mass Destruction, as well as the need for training, awareness, and information sharing efforts directed at state and local responders on the potential impact of disruptions of critical infrastructures, particularly information and communications, on emergency response efforts.

Enhancing Criminal Deterrence for Acts Targeting Critical Infrastructures

Deterrence plays an important preventative role against attacks on critical infrastructures. Deterrence through the criminal law should be built not only through Federal investigative and prosecutive capabilities, but also on state and local, and international capabilities. It should be built to prevent physical and cyber threats to infrastructures.

Physical Threats

Over 30 major Federal criminal laws may be invoked in response to physical attacks on critical infrastructures, and the statutes confer adequate investigative jurisdiction and authority in the vast majority of instances. However, several potential shortfalls remain relating to the ability of this complicated patchwork of laws to deter crimes against critical infrastructures. The Federal Sentencing Guidelines, for example, provide for lighter sentencing for attacks against property, however serious. More severe sentences are reserved for attacks against people and attacks using traditional, violent means—such as explosives and firearms. Thus, the Sentencing Guidelines may not adequately take into account the severity of consequential damages arising from attacks on critical infrastructures. For example, damage resulting from the “downstream” effects of a denial of service attack may result in the possibility of disproportionately light sentences for some forms of attack on critical infrastructure. (*See Adequacy of Criminal Law and Procedure (Physical).*) Accordingly, conclusions can be drawn that:

- The U.S. Sentencing Commission should expand its Sentencing Guidelines to include greater flexibility to address actual and consequential damages, including “downstream” damage to property or loss of service that might result from attacks on critical infrastructures; and

- The Sentencing Commission should consider expanding coverage of Guidelines to make available stricter penalties for uses of biological and chemical weapons not resulting in death.

Two potential deficiencies were identified with respect to purely *intrastate* attacks against critical infrastructures—even when such attacks result in severe damage. In these instances, in order legally to assume jurisdiction over an investigation or prosecution, the Federal government must demonstrate that the incident affects interstate commerce. This may be a particularly difficult determination to make at the earliest stages of an investigation, before the scope of an attack or its effects are well known. Accordingly, a conclusion can be drawn that:

- Congress should consider making a finding that certain critical infrastructures are "instrumentalities of interstate commerce" to help ensure the immediate availability of Federal law enforcement authorities to respond to crimes against those infrastructures and subject those convicted to stiffer Federal penalties. Congress should consider which of the critical infrastructures should be included in such a finding and establish an appropriate nexus between those infrastructures and interstate commerce for inclusion in appropriate legislation.

Legislation that offers reward monies for information leading to the capture of terrorists was reviewed. Under these legal authorities, Congress authorizes the Attorney General and the Secretary of State to administer rewards and payment-for-information programs. It was found that these laws effectively supplement other Federal criminal legislation to protect critical infrastructures, but further research revealed that these programs might be more effectively administered if included as line items in participating agencies' budgets. Accordingly, a conclusion can be drawn that:

- Monetary reward programs for information leading to capture and arrest of criminals should be included as a line-item in participating Federal agencies' budgets to ensure proper funding and implementation of such programs.

Cyber Threats

Efforts are ongoing, within many states, to keep current effective computer crime legislation. Many have produced statutes complete with civil remedies, restitution, forfeiture and special sentencing provisions that may provide needed deterrence in the area, particularly with respect to particular classes of offenders such as juveniles. Prosecution and rehabilitation of juveniles has been predominantly a state and local responsibility. Some states have adopted novel approaches specifically tailored to the unique nature of the crime and the maturity of the offenders. Other states and the federal government can learn from state efforts in this area, and can consider modifications to their laws to address what may be a growing problem. (*See Adequacy of Criminal Law and Procedure (Cyber).*) Accordingly, a conclusion to pursue would be that:

- The Department of Justice sponsor a comprehensive study aimed at compiling demographics of computer crime offenders, comparing the effectiveness of various state approaches to computer crime and discovering effective ways of deterring and responding to computer crime and abuse by juveniles.

The recent approach adopted by the U.S. Sentencing Commission in revising Sentencing Guidelines that apply to violations of the Computer Fraud and Abuse Act was recognized during these studies. The Sentencing Commission expanded applicable definitions of “harm” and “loss” to include interruptions in service; disruptions or delays in delivery of vital services endangering lives; invasions of privacy; and the cost to the victim of damage assessment, restoration of service and data, and loss of business revenue due to interruption of service. It may be advisable to expand this approach to sentencing and sentencing enhancement for possible application in conjunction with the full range of charges that might be implicated by abuse of computers and computer networks, including but not limited to violations of the Wire Fraud statute, the Wiretap statute, the Electronic Communications Privacy Act, or Fraud Relating to Access Devices. Accordingly, a conclusion is that:

- The Sentencing Guidelines Commission consider expanding the application of its broader reformulation of harm and loss (in Guidelines Section 2B1.1, as it applies to violations of the Computer Fraud and Abuse Act and theft of trade secrets) to other forms of electronic crime and crimes relating to information and information technology.

The Department of Justice is currently exploring ways to ease undue administrative burdens on Federal law enforcement officers investigating various forms of computer and high technology crimes that cross Federal jurisdictional boundaries. Law enforcement investigators are currently required to obtain court orders or warrants in many jurisdictions through which a communication might pass or even where electronic information is physically stored. A nationwide capability might allow these procedures to be conducted across jurisdictional boundaries with the authorization of only one Federal judge. These studies bring a recognition of a need for capabilities that, without altering existing processes, would allow for court orders obtained in one jurisdiction to be used in multiple jurisdictions. The Administration and Congress should also be sensitive to such needs, given the value of a rapid law enforcement response. (This conclusion is based on the understanding that this would not constitute an expansion of law enforcement’s current ability to perform these functions, but that modifications would merely increase the speed and efficiency by which existing law enforcement capabilities are administered.) Accordingly, a conclusion emerges that:

- The Administration could endorse and promote efforts currently underway to develop specific procedural changes to assist law enforcement in the investigation of computer crimes, including modification of existing procedures to create effective cross-jurisdictional trace and search warrant capabilities, and that Congress expeditiously consider enactment of such legislation.

The U.S. has been a forerunner among other nations in efforts to clarify and improve current law enforcement procedures pertaining to computer crime. The Administration and Congress could continue to recognize and support these international efforts. This may require, for example, careful comparison of existing standards and procedures for searching and intercepting electronic data during an investigation, as well as support of internationally focused efforts to assure that other countries have the legal and technical capability to conduct and assist in computer crime investigations. Second, the United States could continue with efforts to establish a strong network of international law enforcement agencies and telecommunications carriers to draw on in investigations. The creation and maintenance of such a network can facilitate prompt trace and identification of foreign sources of intrusions. Third, the United States could continue to promote efforts to enhance international cooperation in computer crime investigations, whether through new international arrangements or traditional mutual legal assistance treaties. The U.S. could further ensure that existing and future efforts cover the broadest range of potential sources of attack (i.e. where possible, agreements should cover more than members of recognized multi-lateral organizations). Accordingly, conclusions are drawn that:

- The efforts of U.S. delegations to several international bodies could be acknowledged and fully supported as contributing to infrastructure assurance. Potential areas for continued or expanded efforts in the international area should be highlighted. Specifically:
 1. The U.S. should continue to act as an international leader in efforts to clarify and improve current procedures for investigating computer crime;
 2. The U.S. could work to create a network of international law enforcement agencies and telecommunications carriers to draw on in the course of international investigations of computer crimes; and
 3. The U.S. could continue to promote efforts to enhance international cooperation in computer crime investigations through treaties and other cooperative arrangements both through existing international fora and with countries not represented in those organizations.

Legal Impediments to Vulnerability Assessments

Existing laws may create unnecessary legal impediments to the performance of vulnerability assessments on federal computer systems. The Computer Fraud and Abuse Act criminalizes a wide variety of misconduct premised on unauthorized access to government (and private) computer systems. The legislation is silent, however, as to what might constitute valid authorization for security teams to attempt penetrations without running afoul of the criminal law. Legislative change does not appear to be required, but agencies could clarify attendant

procedures to facilitate sound vulnerability assessment practices. Accordingly, a conclusion is that:

- Agency Chief Information Officers could establish procedures for obtaining expedient and valid authorization to allow vulnerability assessments to be performed on government computer systems. This would require a clear designation by government agencies regarding who may authorize access to their computer systems for this purpose.

Enabling Private Sector Response

Federal authorities that could be strengthened or expanded to allow the Federal government to more adequately accomplish infrastructure assurance objectives were reviewed for the *Legal Foundations* studies. Potential legal impediments that might prevent owners and operators from taking appropriate action to safeguard portions of critical infrastructure within their control and responsibility were also considered. The conclusions contained in this section focus on providing owners and operators greater ability to take protective action.

Additional Deterrence against Cyber Crimes

Deterring cyber-related acts targeting critical infrastructures requires an understanding of the unique nature of this sort of crime. The disparate motivations of the offenders, the continual growth of technologies for committing such crimes, and the decreasing importance of geographic and legal boundaries complicate the application of criminal law to these acts. Many states, the U.S. Congress, the Administration and international bodies have been paying considerable attention to computer crime over the past five years. The result has been improvements in the substantive criminal law, sentencing provisions, investigative procedures and international cooperation. But there is room for more progress. New solution options should be considered to address investigative difficulties and complexities arising in international investigations. Traditional procedures have proven less than effective in responding to the jurisdictional challenges connected with computer crime cases. (*See Approaches to Cyber Intrusion Response.*)

Clearly the capability to do harm and the availability of powerful intrusion tools will continue to grow. Accordingly, there is a need for more powerful ways of deterring criminal behavior. We also have reaffirmed, however, that victims are limited in their ability to detect unauthorized

intrusions and in their willingness to report intrusions, once detected, to law enforcement. This has led to a question of the degree to which the threat of a criminal prosecution currently serves to deter would-be computer criminals, and has prompted analysis of ways to increase the effectiveness—hence the deterrent value—of a law enforcement response. Further complicating deterrence is the ability of intruders to span several traditional legal jurisdictions, which exacerbates the difficulties facing local and state response in this cyber-dimension.

These jurisdictional issues may place a tremendous burden on a centralized law enforcement response. Given the highly resource-intensive and time consuming nature of computer intrusion investigations, this centralized response could quickly be taxed by increases in computer intrusion activity, increases in detection, or even increases in reporting. (Consider, for example, the decentralized mechanisms that developed in response to the growth of automobile transportation, and the corresponding need for enforcement of traffic and parking laws. Similarities are apparent: pervasiveness of rights of way, differing rules governing bodies in motion and at rest). This led to an examination of ways to supplement investigative and prosecutive capabilities to increase deterrence.

Supplementing Investigative Capabilities

The growing use of private responsive capabilities has fueled a rapidly expanding industry of cyber-security specialists and cyber investigative services. In addition, state-licensed private investigators are taking on additional responsibilities in the cyber world. While these services fulfill vital needs of many victims for confidentiality and control, potentially valuable information useful to assessing the scope and nature of the threat is lost in the process. Further, these sensitive duties are being performed by individuals whose qualifications, methods and accountability are unproven. Accordingly, a conclusion can be reached that:

- Congress consider encouragement of increased sharing of information relevant to the scope and nature of the threat, through new ways of facilitating the natural growth of private sector cyber-investigative capabilities.

One possibility might be to consider nationwide licensing of private security specialists under conditions mutually beneficial to the growth of the industry and the development of a predictive threat warning capability. Professional licensing could facilitate responsible growth of the profession by ensuring that trained, qualified and fully insured personnel are available to perform these sensitive duties. Professional licensing could also accelerate the establishment of much-needed industry standards and best practices, and can even serve the interests of privacy by making practitioners more accountable. The licensing body might also facilitate the passing of relevant information in the interests of government and private parties, while meeting clients' needs for confidentiality and control over routine investigations.

The expected growth in incidents requiring investigative response, and formation of effective partnerships between responders may free law enforcement resources for more efficient and targeted use. The availability of private professionals would not interfere with law enforcement's

ability to investigate any incidents that come to or are brought to its attention. With private professionals providing a supplemental response, law enforcement might be freed from the weight of preliminary work associated with distinguishing between nuisance intrusions and real threats, such as dangerous intrusions into federal government systems or incidents involving economic espionage.

It is foreseeable that law enforcement reporting might actually increase, as professional practitioners, reluctant to exceed their legal authority and risk sanction or loss of license, would be inclined to encourage clients to make proper referrals to law enforcement when available private response options have been exhausted.

Supplementing Prosecutive Capabilities

A logical complement to expanding investigative capabilities would be to expand the ability of intrusion victims to proceed in civil actions. Civil remedies are currently available for violations of the Federal Computer Fraud and Abuse Act, though they have rarely been exercised. The interests of deterrence might be served, however, by making civil penalties enforceable internationally through appropriate multilateral mechanisms and agreements. Accordingly, a conclusion from this study is that:

- The President could seek to expand the availability of civil remedies for computer-related violations through appropriate international bodies, multilateral and bilateral agreements.

Countering the “Insider” Threat

Enabling an effective and reliable private intrusion response and an international civil remedy for computer crime are just two ways to help owners and operators to take greater action to protect the critical infrastructures. Another important area relates to the insider threat.

Insiders arguably pose the most immediate and credible threat to the nation’s critical infrastructures. The Federal government is able to guard against misdeeds by insiders to some degree by virtue of its authority to conduct background investigations, issue security clearances, and conduct periodic reinvestigations. The private employers who are the owners and operators of the critical infrastructures often do not have the same ability to screen applicants for certain highly critical positions, or to re-investigate current employees prior to placement in such positions.

Employee Screening

*In the vast majority of instances, an individual employees' interests are likely to outweigh the need for the enhanced security available through rigorous employee screening. But there may be some positions of such sensitivity within the critical infrastructures that security concerns could call for the availability of heightened screening procedures. Reconsideration of existing laws that hinder an employer from obtaining, with the consent of the applicant or employee, certain job-related background information may need to be reconsidered in light of infrastructure assurance concerns.*⁴

Currently, in some states, private employers are unable to get access to criminal history information, are prohibited from requesting or using criminal, financial or employment information, and must avoid tort liability for sharing unfavorable employment history. These restrictions have come about as a result of state and Federal concerns over privacy, fair employment, or rehabilitation of criminals, among others. (*See Privacy Laws and the Employer-Employee Relationship.*) Accordingly, the conclusions which emerge are:

- The Attorney General could convene a group of professionals from law, state and federal legislatures, labor and management organizations and the privacy community to explore existing laws governing employer-employee relations in light of infrastructure assurance objectives. This group could also recommend measures to achieve an appropriate balance between the needs for critical infrastructure owner and operators to conduct appropriate employee background investigations with individual employees' interests in personal privacy; and
- State legislatures could consider adopting "consent" as a baseline for allowing employers to request background information from employees and potential employees for sensitive positions within critical infrastructures, subject to fair information practices.

The group convened by the Attorney General will be in the best position to identify the potential impediments to adequate employee screening for highly sensitive positions. It can also determine which of the critical infrastructures may be in need of such heightened protections and which positions within those infrastructures should be subject to such screening procedures. These recommendations may take the form of model legislation, guidelines, or even preemptive Federal legislation. While this group is studying this issue, the states may wish to examine their laws in light of infrastructure assurance concerns that we have raised and to determine whether they adequately provide for consent as a baseline.

Polygraph Examinations

⁴ In such instances, it is *not* the intention here to mandate such procedures, or even to advocate their use, but to increase the availability of such procedures to certain owners and operators who feel compelled to invoke them. Additionally, any information so obtained would be have to be used in accord with fair information practices.

Another area that would benefit from re-examination in light of infrastructure assurance concerns and the potential risks from insiders is the Employee Polygraph Protection Act (EPPA). Federal law currently prohibits private employers from requiring or even asking employees to submit to polygraph examinations except under very narrow and carefully described circumstances involving an investigation into employee wrongdoing. A second narrow exception exists for employers in certain security professions—so that security companies, such as those that provide armored car services or alarm system installation services to specially enumerated businesses, can periodically polygraph their employees (again, subject to carefully defined conditions and circumstances). But the same rationale that militates in favor of having this exception available for providers of *physical security services* should apply with equal force to providers of *information security services*. This approach is entirely consistent with the Commission’s orientation to remain vigilant to both physical and cyber security issues. Accordingly, a conclusion can be drawn that:

- Congress narrowly expand existing exemptions to the Employee Polygraph Protection Act (EPPA) to include within the scope of its exemptions those who are in the business of providing information security services.

Note that this conclusion neither advocates nor endorses the use of polygraph examinations by employers. It merely seeks for Federal law to extend equal treatment to both physical and cyber-security specialists. There are probably other many other areas of the law that would benefit from being examined and considered for similar treatment.

Enabling Government-Industry Partnership

Infrastructure assurance attempts to bring together diverse interests of the Federal and state and local governments, owners and operators of the infrastructures, and users of infrastructure services. Some of the functions that need to be performed for infrastructure assurance are best performed by those who own and operate the critical infrastructures. Others should be carried out by the government. However, even the most productive efforts of the private sector alone and the government alone will leave a significant void where only joint action will accomplish desired goals. The most prominent example is information sharing. An information sharing mechanism that depends solely on government information or private sector information will only represent part of the picture.

Legal Impediments to Information Sharing

The success of an information sharing mechanism for infrastructure assurance will in large part depend on the creation of a trusted environment where participants, both government and private sector, are encouraged to share sensitive information on a voluntary basis. Several legal impediments currently exist that may prevent or discourage such participation. Impediments to government and private sector participation include apprehension over potential antitrust liability, tort liability, national security concerns, classification of information, legal processes compelling public disclosure, and concerns over the protection of proprietary and trade secret information. These impediments are implicated to varying degrees depending on the precise structure of an information sharing mechanism. However, some important observations surfaced concerning these issues generally as a result of the study. (*See Legal Impediments to Information Sharing.*)

Antitrust Liability

Potential contributors of information from outside of government have often expressed reluctance to participate in the sharing of specific threat and vulnerability information because of impediments they perceive to arise from antitrust and unfair business practice laws. Accordingly, a conclusion drawn is that:

- The Department of Justice could offer limited assurances to the private sector that participation in recognized information sharing processes would not, at least under certain conditions, run afoul of such laws, and consider providing appropriate guidelines to inform such participation.

Tort Liability

The creation of and participation in an operational threat-warning capability may raise liability concerns over failure to share certain information that might have otherwise prevented harm to a critical infrastructure. These failures could carry liability consequences for public and private participants. Determinations such as these, however, are highly dependent on the respective roles and responsibilities of those engaged in the information sharing and threat warning process, and how those roles and responsibilities are specifically delineated. For this reason, any complete study of these operational liability issues must necessarily be performed concurrent with the design of the information sharing capability itself. Accordingly:

- The Federal government could undertake a detailed study of the liability issues which may arise surrounding both government and private sector participation in an infrastructure assurance-related information sharing process.

National Security

With increases to the globalization of business and communications come heightened concerns over the sharing of sensitive information. Currently, many Federal agencies have specific guidelines controlling interaction with foreign corporations or corporate entities with significant foreign ownership. These guidelines, regulations and authorities reflect a variety of disparate approaches. Accordingly:

- The National Security Council could study whether the Federal government should standardize its approaches to and guidelines for sharing information with foreign corporations in light of potential national security benefits and increased government efficiency.

Meanwhile, to facilitate sharing of information for infrastructure assurance purposes, it is vital that a public-private information sharing mechanism establish and adopt appropriate guidelines for sharing information with foreign corporations. Accordingly:

- In the short term, the National Office could set guidelines for the sharing of infrastructure threat and vulnerability information with foreign corporations.

Confidential Information

The Freedom of Information Act and other related laws control the conditions under which information in the possession of the federal government can be made available to the public. Potential participants in an information sharing mechanism may require some degree of assurance that the sensitive information they contribute will remain confidential if shared with the Federal government. Accordingly:

- Appropriate protection of specific private-sector information could be required by, for example, inclusion of a b(3) FOIA exemption in enabling legislation.

Classified Information

Classification issues may arise due to the need to continue to protect classified information in the possession of the government—the contents of which might contribute substantially to a threat warning capability. Accordingly:

- The need for classification of certain information, or certain bodies of aggregated information, and the impact that classification would have on the dissemination process should be considered by the Federal government offices responsible for critical infrastructure assurance.

Trade Secret And Proprietary Information

If appropriate mechanisms for protecting proprietary and trade secret information are not incorporated as part of an information sharing mechanism for infrastructure assurance, private sector participants will be reluctant to share sensitive information. Accordingly:

- The National Office could require appropriate protection of information containing trade secrets or other forms of proprietary information.

State Government Participation

Many of the legal impediments to information sharing identified at the Federal level exist at the state level as well. These include issues regarding liability for participation in information dissemination and the effects of state laws and regulations requiring public access to government information. The great diversity between state laws further complicates any efforts to facilitate and maximize state government participation in information sharing. Accordingly:

- A study group could research and identify legal impediments to information sharing at the state level and propose solutions and draft model legislation to maximize state government participation in information sharing.

Part Four

Infrastructure Assurance, Law and Culture

The conclusions emerging from these studies are intended to help government and the owners and operators of the critical infrastructures do what is needed to achieve enhanced infrastructure assurance. They suggest actions by the Federal government, the private sector, and, where appropriate, by the government and private sector in partnership.

This work was intended to lay a foundation for a gradual process of legal reform. The tools identified through the preparation of the twelve studies and two special studies, and the roles suggested by the conclusions may prompt action by necessary parties. Those who are most closely and intimately involved in these areas, and ultimately in the best position to effect change, to reexamine the laws, regulations and policies under which they operate will find these studies most useful.

A technical definition of “infrastructure assurance” has guided this legal inquiry. Under this definition, infrastructure assurance refers to the “surety of readiness, reliability and continuity of infrastructures such that they are (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in the event of a disruption or attack, and (3) can be readily reconstituted to reestablish vital capabilities.” This definition has served well for compiling relevant authorities, parsing issues, and developing recommendations. Such a technical definition may not be as effective a platform for implementation of concepts and achievement of objectives. Infrastructure assurance is a dynamic set of processes that include individual and shared responsibilities across government and private sectors and, thus, demand implementation through a long-term series of gradual reforms, behavioral reforms, and corresponding legal reforms. In short, it requires cultural change, which results only from changes in behavior.

Viewed in terms of cultural change, “infrastructure assurance” will see businesses respond by including emerging threats and vulnerabilities in their risk management methodology; governments respond by organizing themselves in such ways as to be more able to detect and, in appropriate circumstances, respond to emerging threats and vulnerabilities; and even private citizens, in their homes and offices, modify the way that they practice computer and information security.

The legal community has a responsibility to remain vigilant to these dynamic changes, and to insure that laws facilitate and do not unduly impede it. The conclusions set forth here are the

beginnings of a gradual process, one that must take hold at the local, state, Federal and international levels.